TITLE OF THE INVENTION

デジタルデータ配信システム

BACKGROUND OF THE INVENTION

1) FIELD OF THE INVENTION

本発明は、ネットワークを介してデジタルデータを有料販売する電子商取引（Electronic Commerce）を実現するデジタルデータ配信システムに関する。

2) DESCRIPTION OF THE RELATED ART

ネットワークを介した電子商取引では、一般に情報提供者が開設したホームページに消費者がアクセスし、好みのデジタルデータを選択し、購入処理を行いダウンロードを行う。ダウンロードされたデジタルデータは、ネットワークを通じて違法に二次配布されることを防ぐために、暗号化などの著作権を保護する処理を施される。

以下従来のデジタルデータ配信システムの一例を、図１を用いて説明する。

配信されるデジタルデータは、暗号化された状態で、情報提供者が運用している配信サーバー１０１内の、配信デジタルデータ記録手段１０５に記録されている。その復号鍵と、暗号化デジタルデータ自体の記録場所情報と、そのデジタルデータの利用条件情報は、デジタルデータ管理データベース１０４に記録されている。利用条件情報は、例えば、ダウンロード後のデジタルデータは３回だけ他の記録媒体にコピーすることを許可するといった情報である。

消費者は、受信端末１０２を操作して、送受信手段１０８、通信手段１０９を通じて、配信サーバー１０１にアクセスする。

配信フロントエンド１０６は、デジタルデータ管理データベース１０４の情報に基づいて作成された、配信用音楽デジタルデータの一覧情報を、受信端末１０２に送信する。消費者はブラウズ手段１１０を用いてその一覧情報を閲覧し、配信を希望するデジタルデータがあると、そのデジタルデータの購入要求とユーザー名を配信サーバー１０１に送信する。配信フロントエンド１０６は、送信されたユーザー名が、ユー

ザー管理データベース１０３に含まれていない場合、クレジットカード番号などの支払い情報の入力要求をブラウズ手段１１０に行う。消費者はブラウズ手段１１０を通じて要求されている支払い情報を入力し、配信サーバー１０１に送信する。配信フロントエンド１０６は同支払い情報をユーザ管理データベース１０３に記録し、支払い処理を行う。ユーザー名が、ユーザー管理データベース１０３に含まれている場合には、ユーザー管理データベース１０３に記録されている支払い情報を用いて、支払い処理を行う。支払い処理が正常に処理されると、配信フロントエンド１０６は、デジタルデータ配信手段１０７にたいし、配信を要求されているデジタルデータを、受信端末１０２へ送信するよう指示する。デジタルデータ配信手段１０７は、配信デジタルデータ記録手段１０５から指示されたデジタルデータを、デジタルデータ管理データベース１０４から同デジタルデータの復号鍵と利用条件情報を取り出し、受信端末１０２へ送信する。デジタルデータ管理手段１１１は、受信したデジタルデータをデジタルデータ記録手段１１３に記録し、受信した復号鍵と利用条件情報を、セキュア情報記録手段１１２に記録する。セキュア情報記録手段１１２では、これらのデータを、受信端末１０２に関連付けられた情報で暗号化して記録している。

また、ユーザーが、受信端末１０２上で、デジタルデータを再生する場合、デジタルデータ管理手段１１１は、暗号化された状態のデジタルデータを記録媒体１１３から読み出し、その復号鍵をセキュア情報記録手段１１２から読み出して、デジタルデータの復号化を行う。

また、記録媒体１１４に書き込まれたデジタルデータを、他の可搬性の記録媒体１１７にコピーする場合、まず、デジタルデータ管理手段１１１は、セキュア情報記録手段１１２に記録されている利用条件情報と、過去にコピーした回数情報であるコピー履歴情報を参照し、デジタルデータのコピーを行っても良いかどうかを判定する。デジタルデータ管理手段１１１がコピーを行っても良いと判定した場合、媒体アクセス処理制御手段１１４は、デジタルデータ管理手段１１１から、デジタルデータと、その復号鍵を受け取り、記録媒体アクセス手段１１６を介して、記録媒体１１７にコピーする。この際、復号鍵については、媒体ＩＤ検出手段１１５によって検出された、

記録媒体１１７固有のＩＤである媒体ＩＤ１１８を利用して暗号化した上でコピーを行うものとする。記録媒体１１７へのデジタルデータのコピーが完了すると、デジタルデータ管理手段１１１は、セキュア情報記録手段１１２に記録されているコピー履歴情報を１増やす。

このように従来の技術では、配信サーバーではユーザー情報のみをデジタルデータ配信制御に利用し、受信端末では、デジタルデータの復号鍵、デジタルデータの利用権利情報、およびデジタルデータの利用履歴情報を通常の消費者の操作ではアクセスすることのできない特別なセキュア情報記録手段１１２で管理する。

また、このような従来のデジタルデータ配信システムは、悪意のある消費者から、例えばデジタルデータの配信サーバー１０１からの違法入手や、受信端末１０２に配信されたデジタルデータの違法二次配布等のハッカー行為を受ける可能性が常にある。そのため、特に、デジタルデータの権利管理を行う部分（デジタルデータ管理手段１１１、セキュア情報記録手段１１２）、および、記録媒体へのデジタルデータのコピーを安全に行う記録媒体へのインターフェース部分(媒体アクセス処理制御手段１１４、媒体ＩＤ検出手段１１５）については、タンパレジスタント技術が多かれ少なかれ施されている。

しかしながら上記従来の構成では、受信端末内でのタンパレジスタント技術の実装が必要不可欠であり、以下のような課題を有していた。

タンパレジスタント技術は、それを施す対象となる端末の構成に密接にかかわる。その為、例えば、構成の異なる複数の端末が存在する場合などには、端末毎に、タンパレジスタント技術の開発を行う必要が生じる。これは、端末を製造・販売するメーカーにとっては、非常に負担となる。また、デジタルデータの配信サービスを行う業者にとっても、新しいサービスを開始しようとする際に、構成の異なる複数の受信端末において、そのサービスを受信できるようにする為には、それぞれの受信端末に対してタンパレジスタント技術を開発しなくてはいけないということになると、新しいサービスを開始しにくい。

SUMMARY OF THE INVENTION

本発明は、このような状況に則して考えられたものであって、デジタルデータの権利管理をサーバーで行い、かつ、記録媒体へのインターフェース部分を、記録媒体へアクセスするアダプタ内で実装することによって、受信しようとするサービスに対応したアダプタを接続することで、構成の異なる複数の受信端末においても、その構成の違いを意識することなく、同じように、各種サービスを受信することが可能となるシステムを提供することを目的とする。

以上のような課題を解決するため、本発明の請求項１のデジタルデータ配信システムは、

デジタルデータを配信する配信サーバーと、

配信サーバーから配信されるデジタルデータを受信する受信端末と、

受信端末が受信したデジタルデータの書き込み先となる記録媒体と、

受信端末が受信したデジタルデータを記録媒体へ書き込むアダプタと

によって構成され、

受信端末は、

配信サーバーにアクセスするための通信手段と、

配信サーバーから送られてくる情報を閲覧しそれに応答するためのブラウズ手段と、

アダプタとの接続を制御するアダプタ接続制御手段と

を有し、

記録媒体は、改竄不可能な、その記録媒体を一意に識別することのできる固有の情報である媒体ＩＤを有し、

アダプタは、

セキュア通信手段と、

そのアダプタを一意に識別することのできるアダプタＩＤと、

アダプタＩＤを抽出し、配信サーバーへ送信するアダプタＩＤ検出手段と、

記録媒体から、媒体ＩＤを抽出し、配信サーバーへ送信する媒体ＩＤ検出手段と、

記録媒体にたいしてデータの読み書きを行う記録媒体アクセス手段と、

記録媒体アクセス手段による記録媒体への読み書きを制御する媒体アクセス処理制御手段とを有し、

配信サーバーは、

セキュア通信手段と、

情報やデジタルデータを受信端末に送受信するための送受信手段と、

ユーザーへ送信する情報の生成およびユーザーからのアクセスを処理する配信フロントエンドと、

ユーザーＩＤと関連するユーザーのアカウント情報を記録するユーザー管理データベースと、

配信するデジタルデータの利用条件や格納場所の情報を記録するデジタルデータ管理データベースと、

各ユーザーが取得しているデジタルデータの配信を受ける権利に関する情報を記録する取得済権利管理データベースと、

ユーザーが過去に配信を受けたデジタルデータに関する情報を記録する履歴データベースと、

各ユーザーが使用しているアダプタのアダプタＩＤを記録するアダプタ管理データベースと、

各ユーザーが使用している記録媒体の媒体ＩＤを記録する記録媒体管理データベースと、

暗号化されたデジタルデータと、暗号化されたデジタルデータを復号する復号鍵を記録する配信デジタルデータ記録手段と、

配信デジタルデータ記録手段に記録された復号鍵を、媒体ＩＤ検出手段から送られてくる媒体ＩＤを利用して暗号化する鍵暗号化手段と、

配信フロントエンドからの指示に基づいて、受信端末にたいし、配信デジタルデータ記録手段に記録された暗号化されたデジタルデータと、鍵暗号化手段によって暗号化された復号鍵とを送信するデジタルデータ配信手段とを有し、

アダプタ内のセキュア通信手段と、配信サーバー内のセキュア通信手段は、互いに通

信しあい、アダプタと配信サーバー間にセキュアな通信経路を構築し、
アダプタ内の各構成要素と、配信サーバー内の各構成要素との通信は、セキュア通信手段によって構築されたセキュアな通信経路を使用して行われ、
配信フロントエンドは、
アダプタＩＤ検出手段から送信されてくるアダプタＩＤを利用して、ユーザーの認証を行い、
認証したユーザーからの、デジタルデータ配信要求に対して、取得済権利管理データベースと、履歴データベースと、デジタルデータ管理データベースと、記録媒体管理データベースの情報を参照して、配信要求されたデジタルデータが配信可か否かを判定し、処理を行うとしている。

　また、本発明の請求項２のデジタルデータ配信システムは、
デジタルデータを配信する配信サーバーと、
配信サーバーから配信されるデジタルデータを受信する受信端末と、
受信端末が受信したデジタルデータの書き込み先となる記録媒体と、
受信端末が受信したデジタルデータを記録媒体へ書き込むアダプタと
によって構成され、
受信端末は、
配信サーバーにアクセスするための通信手段と、
配信サーバーから送られてくる情報を閲覧しそれに応答するためのブラウズ手段と、
アダプタとの接続を制御するアダプタ接続制御手段と
を有し、
記録媒体は、改竄不可能な、その記録媒体を一意に識別することのできる固有の情報である媒体ＩＤを有し、
アダプタは、
セキュア通信手段と、
そのアダプタを一意に識別することのできるアダプタＩＤと、
アダプタＩＤを抽出し、配信サーバーへ送信するアダプタＩＤ検出手段と、

記録媒体から、媒体ＩＤを抽出し、配信サーバーへ送信する媒体ＩＤ検出手段と、
鍵暗号化手段と、
記録媒体にたいしてデータの読み書きを行う記録媒体アクセス手段と、
記録媒体アクセス手段による記録媒体への読み書きを制御する媒体アクセス処理制御手段とを有し、
配信サーバーは、
セキュア通信手段と、
情報やデジタルデータを受信端末に送受信するための送受信手段と、
ユーザーへ送信する情報の生成およびユーザーからのアクセスを処理する配信フロントエンドと、
ユーザーＩＤと関連するユーザーのアカウント情報を記録するユーザー管理データベースと、
配信するデジタルデータの利用条件や格納場所の情報を記録するデジタルデータ管理データベースと、
各ユーザーが取得しているデジタルデータの配信を受ける権利に関する情報を記録する取得済権利管理データベースと、
ユーザーが過去に配信を受けたデジタルデータに関する情報を記録する履歴データベースと、
各ユーザーが使用しているアダプタのアダプタＩＤを記録するアダプタ管理データベースと、
各ユーザーが使用している記録媒体の媒体ＩＤを記録する記録媒体管理データベースと、
暗号化されたデジタルデータと、暗号化されたデジタルデータを復号する復号鍵を記録する配信デジタルデータ記録手段と、
配信フロントエンドからの指示に基づいて、受信端末にたいし、配信デジタルデータ記録手段に記録された暗号化されたデジタルデータと復号鍵とを送信するデジタルデータ配信手段とを有し、

鍵暗号化手段は、デジタルデータ配信手段によって配信されてくる復号鍵を、媒体ＩＤ検出手段が検出した媒体ＩＤを利用して暗号化し、記録媒体アクセス制御手段は、記録媒体アクセス手段を制御して、鍵暗号化手段が暗号化した復号鍵を、記録媒体へ書き込み、

アダプタ内のセキュア通信手段と、配信サーバー内のセキュア通信手段は、互いに通信しあい、アダプタと配信サーバー間にセキュアな通信経路を構築し、

アダプタ内の各構成要素と、配信サーバー内の各構成要素との通信は、セキュア通信手段によって構築されたセキュアな通信経路を使用して行われ、

配信フロントエンドは、

アダプタＩＤ検出手段から送信されてくるアダプタＩＤを利用して、ユーザーの認証を行い、

認証したユーザーからの、デジタルデータ配信要求に対して、取得済権利管理データベースと、履歴データベースと、デジタルデータ管理データベースと、記録媒体管理データベースの情報を参照して、配信要求されたデジタルデータが配信可か否かを判定し、処理を行うとしている。

　また、本発明の請求項３のデジタルデータ配信システムは、

デジタルデータを配信する配信サーバーと、

配信サーバーから配信されるデジタルデータを受信する受信端末と、

受信端末が受信したデジタルデータの書き込み先となる記録媒体と、

受信端末が受信したデジタルデータを記録媒体へ書き込むアダプタと

によって構成され、

受信端末は、

配信サーバーにアクセスするための通信手段と、

配信サーバーから送られてくる情報を閲覧しそれに応答するためのブラウズ手段と、

アダプタとの接続を制御するアダプタ接続制御手段と

を有し、

記録媒体は、改竄不可能な、その記録媒体を一意に識別することのできる固有の情報

である媒体ＩＤを有し、

アダプタは、

セキュア通信手段と、

そのアダプタを一意に識別することのできるアダプタＩＤと、

アダプタＩＤを抽出し、配信サーバーへ送信するアダプタＩＤ検出手段と、

記録媒体から、媒体ＩＤを抽出し、配信サーバーへ送信する媒体ＩＤ検出手段と、

暗号変換手段と、

鍵暗号化手段と、

記録媒体にたいしてデータの読み書きを行う記録媒体アクセス手段と、

記録媒体アクセス手段による記録媒体への読み書きを制御する媒体アクセス処理制御手段とを有し、

配信サーバーは、

セキュア通信手段と、

情報やデジタルデータを受信端末に送受信するための送受信手段と、

ユーザーへ送信する情報の生成およびユーザーからのアクセスを処理する配信フロントエンドと、

ユーザーＩＤと関連するユーザーのアカウント情報を記録するユーザー管理データベースと、

配信するデジタルデータの利用条件や格納場所の情報を記録するデジタルデータ管理データベースと、

各ユーザーが取得しているデジタルデータの配信を受ける権利に関する情報を記録する取得済権利管理データベースと、

ユーザーが過去に配信を受けたデジタルデータに関する情報を記録する履歴データベースと、

各ユーザーが使用しているアダプタのアダプタＩＤを記録するアダプタ管理データベースと、

各ユーザーが使用している記録媒体の媒体ＩＤを記録する記録媒体管理データベース

と、

第一の暗号化方式で暗号化されたデジタルデータと、第一の暗号化方式で暗号化されたデジタルデータを復号する復号鍵を記録する配信デジタルデータ記録手段と、

配信フロントエンドからの指示に基づいて、受信端末にたいし、配信デジタルデータ記録手段に記録された第一の暗号化方式で暗号化されたデジタルデータとその復号鍵とを送信するデジタルデータ配信手段とを有し、

暗号変換手段は、デジタルデータ配信手段によって配信されてくる第一の暗号化方式で暗号化されたデジタルデータを、デジタルデータ配信手段によって配信されてくる復号鍵を使用して復号化し、復号化したデジタルデータを、第二の暗号化方式によって暗号化し、

鍵暗号化手段は、暗号変換手段がデジタルデータを第二の暗号化方式によって暗号化する際に使用した鍵を、媒体ＩＤ検出手段が検出した媒体ＩＤを利用して暗号化し、

記録媒体アクセス制御手段は、記録媒体アクセス手段を制御して、鍵暗号化手段が暗号化した鍵を、記録媒体へ書き込むことを特徴とし、

アダプタ内のセキュア通信手段と、配信サーバー内のセキュア通信手段は、互いに通信しあい、アダプタと配信サーバー間にセキュアな通信経路を構築し、

アダプタ内の各構成要素と、配信サーバー内の各構成要素との通信は、セキュア通信手段によって構築されたセキュアな通信経路を使用して行われ、

配信フロントエンドは、

アダプタＩＤ検出手段から送信されてくるアダプタＩＤを利用して、ユーザーの認証を行い、

認証したユーザーからの、デジタルデータ配信要求に対して、取得済権利管理データベースと、履歴データベースと、デジタルデータ管理データベースと、記録媒体管理データベースの情報を参照して、配信要求されたデジタルデータが配信可か否かを判定し、処理を行うとしている。

また、本発明の請求項４のデジタルデータ配信制御方法は、

請求項１～３何れかに記載のデジタルデータ配信システムにおいて、

配信フロントエンドが、
アダプタＩＤ検出手段から送信されてくるアダプタＩＤを利用して、ユーザーの認証を行い、
認証したユーザーからの、デジタルデータ配信要求に対して、取得済権利管理データベースと、履歴データベースと、デジタルデータ管理データベースと、記録媒体管理データベースの情報を参照して、配信要求されたデジタルデータが配信可か否かを判定し、処理を行うとしている。

また、本発明の請求項５のデジタルデータ配信システムは、
請求項１～３何れかに記載のデジタルデータ配信システムであって、
アダプタは、前記アダプタ内のセキュア通信手段をアップデートするセキュア通信手段アップデート手段を有し、
配信サーバーは、
配信サーバー内のセキュア通信手段をアップデートするセキュア通信手段アップデート手段と、

必要に応じて、アダプタ内のセキュア通信手段アップデート手段と配信サーバー内のセキュア通信手段アップデート手段に、セキュア通信手段のアップデートを行うよう指示するセキュア通信手段アップデート指示手段とを有する。

BRIEF DESCRIPTION OF THE DRAWINGS

図１は、従来の技術におけるデジタルデータ配信システムの構成の一例を示す図。
図２は、本発明の実施の形態１におけるデジタルデータ配信システムの実現形態の一例を示す図。
図３は、本発明の実施の形態１におけるデジタルデータ配信システムの構成を示す図。
図４は、本発明の実施の形態１における記録媒体の構成を示す図。
図５は、本発明の実施の形態１におけるユーザーアカウント情報データベースの一例を示す図。
図６は、本発明の実施の形態１におけるアダプタ情報データベースの一例を示す図。

図７は、本発明の実施の形態１における記録媒体情報データベースの一例を示す図。
図８は、本発明の実施の形態１におけるサービス種別データベースの一例を示す図。
図９は、本発明の実施の形態１におけるデジタルデータ情報データベースの一例を示す図。
図１０は、本発明の実施の形態１における取得済権利管理データベースの一例を示す図。
図１１は、本発明の実施の形態１における履歴データベースの一例を示す図。
図１２は、本発明の実施の形態１におけるデジタルデータ配信システムの全体の動作の流れを示すフローチャート。
図１３は、本発明の実施の形態１における入会プロセスを説明するフローチャート。
図１４は、本発明の実施の形態１におけるデジタルデータ選択プロセスを説明するフローチャート。
図１５は、本発明の実施の形態１における購読処理プロセスを説明するフローチャート。
図１６は、本発明の実施の形態１における単独販売処理プロセスを説明するフローチャート。
図１７は、本発明の実施の形態１におけるデジタルデータダウンロードプロセスを説明するフローチャート。
図１８は、本発明の実施の形態１における記録媒体正当性チェックプロセスを説明するフローチャート。
図１９は、本発明の実施の形態１における記録媒体書き込みプロセスを説明するフローチャート。
図２０は、本発明の実施の形態１における受信端末がユーザーに提示するログイン画面の一例を示す図。
図２１は、本発明の実施の形態１における受信端末がユーザーに提示するユーザー登録画面の一例を示す図。
図２２は、本発明の実施の形態１における受信端末がユーザーに提示する購読サービ

スデジタルデータ選択画面の一例を示す図。

図２３は、本発明の実施の形態１における受信端末がユーザーに提示する単独販売サービスデジタルデータ選択画面の一例を示す図。

図２４は、本発明の実施の形態１における受信端末がユーザーに提示するダウンロードデジタルデータ選択画面の一例を示す図。

図２５は、本発明の実施の形態１におけるセキュア通信方法更新プロセスを説明するフローチャート。

図２６は、本発明の実施の形態２におけるデジタルデータ配信システムの構成を示す図。

図２７は、本発明の実施の形態２における記録媒体書き込みプロセスを説明するフローチャート。

図２８は、本発明の実施の形態３におけるデジタルデータ配信システムの構成を示す図。

図２９は、本発明の実施の形態３における記録媒体書き込みプロセスを説明するフローチャート。

図３０は、本発明のデジタルデータ配信システムの構成の一例を示す図。

DESCRIPTION OF THE PREFERRED EMBODIMENT

（実施の形態１）

以下、本発明の実施の形態１について、図面を参照しながら説明する。

図２は、実施の形態１におけるデジタルデータ配信システムの実現形態の一例を示す図である。２０１はデジタルデータ配信サービス会社で、デジタルデータの配信を行う配信サーバーを運営している。２０３は、消費者が操作する受信端末であるＳＴＢ（Ｓｅｔ　Ｔｏｐ　Ｂｏｘ）である。２０２はＣａｂｌｅ基地局でデジタルデータ配信サービス会社２０１と消費者の受信端末２０３をＣａｂｌｅ回線で繋ぐ。２０４は、配信されるデジタルデータの書き込み先である記録媒体である。２０５は、受信端末２０３に接続され、受信端末２０３が受信したデジタルデータを、記録媒体２０４へ

書き込む記録媒体アクセスアダプタである。

本実施の形態では、デジタルデータとして音楽デジタルデータの場合を例に説明する。また、デジタルデータ配信システムが提供するサービスとして、１曲ごとに価格が決まっている単体販売サービス、月毎に一定金額を支払えば指定された音楽デジタルデータ群から任意の曲を予め定められた個数までは自由にをダウンロードしてもよい購読サービスと、月毎に一定金額を支払えば指定された音楽デジタルデータ群から制限なく好きな曲をダウンロードしてもよい購読サービスの３サービスを例に説明する。

図３は、本実施の形態におけるデジタルデータ配信システムの構成を示す図である。本実施の形態のデジタルデータ配信システムは、配信サーバー３０１、受信端末３０２、記録媒体アクセスアダプタ３０３から構成される。

配信サーバー３０１は、デジタルデータを配信するサーバーであり、ユーザー管理データベース３０４、デジタルデータ管理データベース３０５、取得済権利管理データベース３０６、履歴データベース３０７、配信デジタルデータ記録手段３０８、配信フロントエンド３０９、デジタルデータ配信手段３１０、送受信手段３１１、セキュア通信手段３１２、セキュア通信方法更新手段３１３、更新制御手段３１４から構成される。

受信端末３０２は、デジタルデータを受信する端末であり、通信手段３１５、ブラウズ手段３１６、アダプタ接続制御手段３１７から構成される。

記録媒体アクセスアダプタ３０３は、そのアダプタを一意に特定することのできる固有のＩＤであるアダプタＩＤ３２６を有し、記録媒体３２７へのデータの読み書きを行うアダプタである。記録媒体アクセスアダプタ３０３は、セキュア通信手段３１８、アダプタＩＤ検出手段３１９、媒体ＩＤ検出手段３２０、暗号変換手段３２１、復号鍵暗号化手段３２２、媒体アクセス処理制御手段３２３、記録媒体アクセス手段３２４、セキュア通信方法更新手段３２５から構成される。なお、本実施の形態においては、記録媒体アクセスアダプタ３０３内の各構成要素は、１つのＬＳＩ（図３の破線で囲まれた部分）のなかに統合されて実装されているとする。

以下、各構成要素について説明する。

ユーザー管理データベース３０４は、ユーザーのアカウント情報を記録するユーザーアカウント情報データベース、ユーザーが所有するアダプタの情報を記録するアダプタ情報データベース、ユーザーが過去配信先として用いた記録媒体の情報を記録した記録媒体情報データベースの３つのデータベースで構成されるリレーショナルデータベースである。　図５はユーザーアカウント情報データベースの一例を示す図であり、ユーザーＩＤ、ログイン名、パスワード、ユーザーの名前、ユーザーの住所、代金を支払うクレジットカードの種類、クレジットカード番号、それにユーザーが加入している音楽配信サービスプラン情報で構成される。図６は、アダプタ情報データベースの一例を示す図であり、このデータベースのインデックス情報であるアダプタ登録ＩＤ、そのアダプタの所持者であるユーザーＩＤ、そのアダプタの種類情報、そしてアダプタＩＤで構成されている。

図７は記録媒体情報データベースの一例を示す図であり、このデータベースのインデックス情報である媒体登録ＩＤ、デジタルデータの配信を受けたユーザーＩＤ、媒体の種類情報、そして媒体ＩＤで構成される。

デジタルデータ管理データベース３０５は、このサイトで販売しているデジタルデータの販売サービスプランが記録されるサービス種別データベースと、デジタルデータ自体の情報、および、デジタルデータの格納場所情報が記録されるデジタルデータ情報データベースで構成される。

図８は、サービス種別データベースの一例を示す図であり、インデックス情報であるあービスＩＤ、サービス名、祖サービスの支払い方法種別である課金種別、サービスの金額、１ユーザーの総ダウンロード曲数の制限情報であるＤＬ総曲数制限、１曲あたりのダウンロード回数の制限情報である曲当りＤＬ回数制限で構成されている。

図９は、デジタルデータ情報データベースの一例を示す図であり、デジタルデータＩＤと、デジタルデータの曲名、アーティスト名、そのデジタルデータが属しているサービスＩＤ、デジタルデータの価格、デジタルデータの格納場所情報で構成される。

取得済権利管理データベース３０６は、ユーザーが得た、デジタルデータを配信さ

れる権利を管理するデータベースである。図１０は、その一例を示す図であり、取得済権利管理データベース３０６は、インデックスである権利ＩＤ、デジタルデータの配信される権利を取得しているユーザーＩＤ、そのデジタルデータのデジタルデータＩＤ、権利を取得した購入日時、デジタルデータが所属しているサービスＩＤで構成される。

履歴データベース３０７は、ユーザーが配信を受けた情報を管理する履歴データベースである。図１１は、その一例を示す図であり、履歴データベース３０７は、インデックスである履歴ＩＤ、対象となる権利ＩＤ、処理を行った日時である処理日時、処理内容、ＤＬ先媒体ＩＤで構成される。

配信デジタルデータ記録手段３０８は、配信するデジタルデータを所定の暗号化方式で暗号化した状態で記録し、その復号鍵も記録する。なお、以降、ここで使用している暗号化方式を、第一の暗号化方式とよぶこととする。

配信フロントエンド３０９は、ユーザーがアクセスするホームページ画面データを生成しユーザーに提供する。また、配信フロントエンド３０９は、生成したホームページ画面データに応じてユーザーが行った操作に応答する処理を行う。

デジタルデータ配信手段３１０は、配信デジタルデータ記録手段３０８に記録されている、暗号化された状態のデジタルデータと復号鍵を、記録媒体アクセスアダプタ３０３へ送信する処理を行う。

送受信手段３１１と通信手段３１５は、配信サーバー３０１と受信端末３０２間の通信処理を行う。なお、この通信は、必要に応じて、SSL（Secure Socket Layer）等、何らかの技術を利用して、セキュアに行われる。

セキュア通信手段３１２とセキュア通信手段３１８は、互いに通信し合い、配信サーバー３０１と記録媒体アクセスアダプタ３０３間にセキュアな通信経路を構築する。なお、配信サーバー３０１内の各構成要素と、記録媒体アクセスアダプタ３０３内の各構成要素との通信は、このセキュアな通信経路を介して行われるものとする。

セキュア通信方法更新手段３１３は、後述する更新制御手段３１４の指示に従って、セキュア通信手段３１２のアップデートを行う。

更新制御手段３１４は、例えば、セキュア通信手段３１２とセキュア通信手段３１８がセキュアな通信経路を構築する際に使用していた方法がハッキングされた場合等に、セキュア通信手段３１２およびセキュア通信手段３１８をアップデートをしその方法を変更するよう、それぞれ、セキュア通信方法更新手段３１３、セキュア通信方法更新手段３２５に対し、指示する。

ブラウズ手段３１６は、ホームページ画面データを表示し、それに対するユーザーの操作を受信し処理する。

アダプタ接続制御手段３１７は、受信端末３０２と記録媒体アクセスアダプタ３０３とを接続し、配信サーバー３０１と記録媒体アクセスアダプタ３０３が、受信端末３０２を介して通信を行えるようにする。

アダプタＩＤ検出手段３１９は、記録媒体アクセスアダプタ３０３に含まれる、アダプタＩＤ３２６を検出し、それを配信サーバー３０１へ送信する。

媒体ＩＤ検出手段３２０は、記録媒体３２７から、後述する媒体ＩＤ３２８を取得し、配信サーバー３０１へ送信する。なお、記録媒体３２７は、図４に示すように、アクセスする際に認証が必要なセキュアデータエリア４０１と、認証が不要なデータエリア４０２とから構成されており、セキュアデータエリア４０１には、その記録媒体を一意に特定することのできるＩＤである媒体ＩＤ３２８が記録されている。

暗号変換手段３２１は、デジタルデータ配信手段３１０から、第一の暗号化方式で暗号化されたデジタルデータとその復号鍵を受け取ると、まず、そのデジタルデータの復号化を行う。次に、復号化したデジタルデータを、所定の暗号化方式で暗号化する。以降、本実施の形態では、ここで暗号化に使用しる暗号化方式のことを第二の暗号化方式とよぶこととする。

復号鍵暗号化手段３２２は、暗号変換手段３２１がデジタルデータを第二の暗号化方式で暗号化した際に使用した鍵を、媒体ＩＤ検出手段３２０が検出した媒体ＩＤ３２８を利用して暗号化する。

媒体アクセス制御手段３２３は、記録媒体３２７にアクセスする手段である記録媒体アクセス手段３２４を制御し、記録媒体３２７へのデータの読み書きを制御する。

媒体アクセス制御手段３２３は、記録媒体アクセス手段３２４を制御し、暗号変換手段３２１が第二の暗号化方式で暗号化したデジタルデータをデータ領域４０２に記録し、また、復号鍵暗号化手段３２２が暗号化した鍵を、セキュアデータエリア４０１に記録する。

セキュア通信方法更新手段３２５は、更新制御手段３１４の指示に従って、セキュア通信手段３１８のアップデートを行う。

以下、各構成要素の動作について、デジタルデータ配信システムが提供する動作ごとに説明を行う。

まず、図１２に示すフローチャートをもとに、デジタルデータ配信システムの全体の動作の流れを説明する。

（Ｓ１２０１）ユーザーは、ブラウズ手段３１６を用い、配信サーバー３０１にアクセスする。

（Ｓ１２０２）配信フロントエンド３０９は、図２０に示すような、ログイン画面のデータを生成し、受信端末３０２に送信する。ブラウズ手段３１６は、ログイン画面を表示する。

（Ｓ１２０３）ここで、ユーザーがこのサービスを受ける会員でない場合、後述する入会プロセスが実行される。

（Ｓ１２０４）ユーザーは、記録媒体アクセスアダプタ３０３が受信端末３０２に接続されていることを確認し、接続されていない場合には接続する。ここで、アダプタ接続制御手段３１７は、受信端末３０２と記録媒体アクセスアダプタ３０３との接続状態を制御して、配信サーバー３０１と記録媒体アクセスアダプタ３０３が、受信端末３０２を介して通信を行えるようにする。その後、ユーザーは、Ｓ１２０２で表示されたログイン画面上で、ユーザー名とパスワードを入力後、Log in ボタンを実行する。Log in ボタンが実行されると、配信サーバー３０１に対し、ブラウズ手段３１６は、入力されたユーザー名とパスワードを送信する。また、アダプタＩＤ検出手段３１９は、アダプタＩＤ３２６を検出し、配信サーバー３０１に送信する。なお、この際の通信は、セキュア通信手段３１２とセキュア通信手段３１８が、互いに通信し

合い構築したセキュアな通信経路を使用するものとする。以降、配信サーバー３０１内の各構成要素と記録媒体アクセスアダプタ３０３内の各構成要素との通信は、基本的に、このセキュアな通信経路を使用して行われるものとする。

（Ｓ１２０５）配信フロントエンド３０９は、Ｓ１２０４で送信されてきたユーザー名、パスワード、アダプタＩＤ３２６をもとに、ユーザー管理データベース３０４を参照し、ユーザーを特定する。その後、配信フロントエンド３０９は、図２２に示すような、先程特定したユーザー用にカスタマイズした、ダウンロードする権利を取得したい曲の選択画面のデータを生成し、受信端末３０２に送信する。なお、Ｓ１２０４で送信されてきた情報が、不正な情報である場合には、配信フロントエンド３０９は、その旨をユーザーに伝え再度ログインを行うことを促す画面データを生成し、受信端末３０２に送信する。

（Ｓ１２０６）図２２に示すような画面上で、ユーザーは、ブラウズ手段３１６を用いて、デジタルデータをダウンロードする権利の取得、既に権利を取得したデジタルデータのダウンロード、ログアウト、のいずれを行うかを選択する。

（Ｓ１２０７）Ｓ１２０６でユーザーが、デジタルデータをダウンロードする権利の取得を選択した場合、後述するデジタルデータ選択プロセスが実行され、その後、Ｓ１２０６に戻る。

（Ｓ１２０８）Ｓ１２０６でユーザーが、既に権利を取得したデジタルデータのダウンロードを選択した場合、後述するデジタルデータダウンロードプロセスが実行され、その後、Ｓ１２０６に戻る。

（Ｓ１２０９）Ｓ１２０６でユーザーが、ログアウトを選択すると、配信サーバー３０１と受信端末３０２との接続は切断され、本プロセスは終了する。

以上で、デジタルデータ配信システムの全体の動作の流れについての説明を終わる。

図１３は、入会プロセスの動作の流れを表す。入会プロセスは、ユーザーが、サービスを受ける会員になるための処理を行うプロセスである。以下、その動作について説明する。

（Ｓ１３０１）配信フロントエンド３０９は、図２１に示すようなユーザー登録画

面のデータを生成し、受信端末３０２に送信する。すると、ブラウズ手段３１６によってユーザー登録画面が表示されるので、ユーザーは、必要事項である、ユーザー名、パスワード、住所、電話番号、支払いクレジットカード情報を記入する。

（Ｓ１３０２）次に、ユーザーは、加入したいサービスを選択する。ここで単独購読サービスは個々の曲購入時に支払いを行うためここで加入処理をする必要はない。ブラウズ手段３１６は、入力された情報を配信サーバー３０１に送信する。

（Ｓ１３０３）次に、配信フロントエンド３０９は、このサービスでデジタルデータの書き込み装置として用る記録媒体アクセスアダプタ３０３を、受信端末３０２に接続するよう促す画面を生成し、受信端末３０２に送信する。ユーザーは、デジタルデータの書き込み装置として用いたい記録媒体アクセスアダプタ３０３を、受信端末３０２に接続する。

（Ｓ１３０４）アダプタＩＤ検出手段３１９は、アダプタＩＤ３２６を検出し、配信サーバー３０１へ送信する。

（Ｓ１３０５）Ｓ１３０２、Ｓ１３０４で送信された情報は、配信フロントエンド３０９により、ユーザー管理データベース３０４に登録される。

以上で、入会プロセスの説明を終了する。

図１４は、デジタルデータ選択プロセスの動作の流れを表す。デジタルデータ選択プロセスは、デジタルデータをダウンロードする権利を、ユーザーが取得するためのプロセスである。以下、その動作について説明を行う。

（Ｓ１４０１）ユーザーは、ブラウズ手段３１６を用いて、受信したいサービスを選択する。

（Ｓ１４０２～Ｓ１４０４）Ｓ１４０１でユーザーが選択したサービスが、購読サービスの場合には、後述する購読処理プロセスが実行される。また、Ｓ１４０１でユーザーが選択したサービスが、単独販売サービスの場合には、後述する単独販売処理プロセスが実行される。

以上で、デジタルデータ選択プロセスの説明を終わる。

図１５は、購読処理プロセスの動作の流れを表す。購読処理プロセスは、選択され

た購読サービスによって配信されるデジタルデータをダウンロードする権利を、ユーザーが取得するためのプロセスである。以下、その動作について説明する。

（Ｓ１５０１）まず、配信フロントエンド３０９は、ユーザー管理データベース３０４を参照し、ユーザーが、選択された購読サービスの会員か否かを検証する。

（Ｓ１５０２）Ｓ１５０１で、ユーザーが会員で無いと判定された場合、配信フロントエンド３０９は、デジタルデータ管理データベース３０５に基づいて、選択されたサービスに属するデジタルデータを一覧表示するが、デジタルデータの選択はできない画面のデータを生成して、受信端末３０２に送信する。ブラウズ手段３１６は、その画面を表示する。

（Ｓ１５０３）この場合、ユーザーはブラウズ手段３１６を用いて、デジタルデータのリストの閲覧のみできる。

（Ｓ１５０４）Ｓ１５０１で、ユーザーが会員であると判定された場合、配信フロントエンド３０９は、取得済権利管理データベース３０６を参照し、選択された購読サービスに含まれるデジタルデータ各々について、ユーザーがダウンロードする権利を取得済みかどうかを調べる。

（Ｓ１５０５）配信フロントエンド３０９は、デジタルデータ管理データベース３０５に基づいて、選択されたサービスに属するデジタルデータを、ユーザーが選択できる状態で一覧表示し、さらに、Ｓ１５０４でダウンロードする権利を取得済みであると判定されたデジタルデータについては、既に取得済のマークを表示する画面のデータを生成し、受信端末３０２に送信する。ブラウズ手段３１６は、その画面を表示する。この画面の一例を図２２に示す。

（Ｓ１５０６）ユーザーは、ブラウズ手段３１６を用いて、取得したいデジタルデータを選択する。ブラウズ手段３１６は、配信サーバー３０１へその情報を送信する。

（Ｓ１５０７）配信フロントエンド３０９は、Ｓ１５０６で送信された情報に基づいて、ダウンロードする権利の取得要求のあったデジタルデータの情報を、取得済権利管理データベース３０６に新規登録する。

以上で、購読処理プロセスの説明を終わる。

図１６は、単独販売処理プロセスの動作の流れを表す。単独販売処理プロセスは、単独販売サービスによって配信されるデジタルデータをダウンロードする権利を、ユーザーが取得するためのプロセスである。以下、その動作について説明する。

（Ｓ１６０１）配信フロントエンド３０９は、取得済権利管理データベース３０６を参照し、単独販売サービスに含まれるデジタルデータ各々について、ユーザーがダウンロードする権利を取得済みかどうかを調べる。

（Ｓ１６０２）配信フロントエンド３０９は、デジタルデータ管理データベース３０５に基づいて、選択されたサービスに属するデジタルデータを、ユーザーが選択できる状態で一覧表示し、さらに、Ｓ１６０１でダウンロードする権利を取得済みであると判定されたデジタルデータについては、既に取得済のマークを表示する画面のデータを生成し、受信端末３０２に送信する。ブラウズ手段３１６は、その画面を表示する。この画面の一例を図２３に示す。

（Ｓ１６０３）ユーザーは、ブラウズ手段３１６を用いて、取得したいデジタルデータを選択する。ブラウズ手段３１６は、配信サーバー３０１へその情報を送信する。

（Ｓ１６０４）配信フロントエンド３０９は、ユーザーがダウンロードする権利の取得要求をだしているデジタルデータの価格を、デジタルデータ管理データベース３０５を参照して計算し、ユーザー管理データベース３０４に登録されているクレジットカード情報等の支払い用の情報を用いて、購入決済処理を行う。

（Ｓ１６０５）配信フロントエンド３０９は、購入決済処理の行われたデジタルデータの情報を取得済権利管理データベース３０６に新規登録する。

以上で単独販売処理プロセスの説明を終わる。

図１７はデジタルデータダウンロードプロセスの動作の流れを表す。デジタルデータダウンロードプロセスは、ユーザーが、デジタルデータをダウンロードするプロセスである。以下、その動作について説明する。

（Ｓ１７０１）まず、配信フロントエンド３０９は、取得済権利管理データベース３０６から、ユーザーがダウンロードする権利を取得しているデジタルデータの一覧を取得する。

（Ｓ１７０２）次に、配信フロントエンド３０９は、Ｓ１７０１で取得した一覧に記載されたデジタルデータ各々について、履歴データベース３０７およびデジタルデータ管理データベース３０５を参照して、そのデジタルデータが、ダウンロード可能であるか、可能な場合、あと何回ダウンロードできるかを判定する。

（Ｓ１７０３）次に配信フロントエンド３０９は、Ｓ１７０２での結果を基に、図２４に示すような､ユーザーがダウンロードする権利を有するデジタルデータの一覧、およびダウンロードできる回数を示した画面データを生成して、受信端末３０２へ送信する。ブラウズ手段３１６は、その画面を表示する。

（Ｓ１７０４）ユーザーは、ブラウズ手段３１６を用い、ダウンロードしたいデジタルデータを選択する。ブラウズ手段３１６は、その情報を配信サーバー３０１へ送信する。

（Ｓ１７０５）次に、媒体ＩＤ検出手段３２０が、記録媒体アクセスアダプタ３０３に装着されている記録媒体３２７の媒体ＩＤ３２８を検出し、配信サーバー３０１へ送信する。

（Ｓ１７０６）配信フロントエンド３０９は、Ｓ１７０５で媒体ＩＤ検出手段３２０が送信した媒体ＩＤ３２８を有する記録媒体３２７について、後述する記録媒体正当性チェックプロセスを実行する。

（Ｓ１７０７）配信フロントエンド３０９は、Ｓ１７０５で媒体ＩＤ検出手段３２０が送信した媒体ＩＤ３２８を有する記録媒体３２７の正当性を検証する。

（Ｓ１７０８）Ｓ１７０７で、記録媒体３２７は正当でないと判定された場合、配信フロントエンド３０９は、記録媒体が不正な可能性がある旨の警告画面のデータを生成し、受信端末３０２に送信する。ブラウズ手段３１６は、その画面を表示する。

（Ｓ１７０９）Ｓ１７０７で、記録媒体３２７は正当であると判定された場合、後述する記録媒体書き込みプロセスが実行される。

（Ｓ１７１０）配信フロントエンド３０９は、デジタルデータがダウンロードされたという情報を履歴データベース３０７に追加する。

以上で、デジタルデータダウンロードプロセスの説明を終わる。

図１８は記録媒体正当性チェックプロセスの動作の流れを表す。記録媒体正当性チェックプロセスは、ユーザーが、デジタルデータを書き込もうとしている記録媒体３２７の正当性をチェックするためのプロセスである。以下、その動作について説明する。

（Ｓ１８０１）配信フロントエンド３０９は、Ｓ１７０５で送信されてきた媒体ＩＤ３２８が、ユーザー管理データベース３０４の記録媒体情報データベースに登録されているものかどうか検証する。配信フロントエンド３０９は、登録されているものであると判定した場合、Ｓ１８０５の処理に進む。

（Ｓ１８０２）Ｓ１８０１で、登録されていないと判定された場合、配信フロントエンド３０９は、同じユーザーが既に使用している記録媒体３２７の個数を、ユーザー管理データベース３０４の記録媒体情報データベースから算出し、その個数が、予め決められた規定数以上かどうかを判断する。

（Ｓ１８０３）Ｓ１８０２で、規定数以上と判定された場合、配信フロントエンド３０９は、チェック対象の記録媒体３２７は正当ではないと判断する。

（Ｓ１８０４）Ｓ１８０２で、規定数未満と判定された場合、配信フロントエンド３０９は、Ｓ１７０５で送信された媒体ＩＤ３２８をユーザー管理データベース３０４の記録媒体情報データベースに追加し、Ｓ１８０５の処理に進む。

（Ｓ１８０５）配信フロントエンド３０９は、チェック対象の記録媒体３２７は正当であると判断する。

以上で、記録媒体正当性チェックプロセスの説明を終わる。

図１９は、記録媒体書き込みプロセスの動作の流れを表す。記録媒体書き込みプロセスは、記録媒体３２７に、デジタルデータおよびその復号鍵を書き込むプロセスである。以下、その動作について説明する。

（Ｓ１９０１）デジタルデータ配信手段３１０は、配信デジタルデータ記録手段３０８に格納されている、ダウンロード要求のあったデジタルデータを、記録媒体アクセスアダプタ３０３へ送信する。

（Ｓ１９０２）デジタルデータ配信手段３１０は、配信デジタルデータ記録手段３

０８に格納されている、ダウンロード要求のあったデジタルデータに対応する復号鍵を、記録媒体アクセスアダプタ３０３へ送信する。

（Ｓ１９０３）暗号変換手段３２１は、Ｓ１９０１でデジタルデータ配信手段３１０が送信したデジタルデータを、Ｓ１９０２でデジタルデータ配信手段３１０が送信した復号鍵を使用して復号化する。

（Ｓ１９０４）暗号変換手段３２１は、Ｓ１９０３で暗号変換手段３２１が復号化したデジタルデータを、第二の暗号化方式で暗号化する。

（Ｓ１９０５）復号鍵暗号化手段３２２は、Ｓ１９０４で暗号変換手段３２１がデジタルデータの暗号化の際に使用した鍵を、媒体ＩＤ検出手段３２０が検出した媒体ＩＤ３２８を利用して暗号化する。

（Ｓ１９０６）媒体アクセス処理制御手段３２３は、Ｓ１９０５で復号鍵暗号化手段３２２が暗号化した鍵を、記録媒体アクセス手段３２４を制御して、記録媒体３２７のセキュアデータエリア４０１に記録する。

（Ｓ１９０７）媒体アクセス処理制御手段３２３は、Ｓ１９０４で暗号変換手段３２１が暗号化したデジタルデータを、記録媒体アクセス手段３２４を制御して、記録媒体３２７のデータエリア４０２に記録する。

以上で、記録媒体書き込みプロセスの説明を終わる。

図２５は、セキュア通信方法更新プロセスの動作の流れを表す。セキュア通信方法更新プロセスは、セキュア通信手段３１２とセキュア通信手段３１８がセキュアな通信経路を構築する際に使用していた方法がハッキングされた場合等に、セキュア通信手段３１２、およびセキュア通信手段３１８をアップデートし、その方法を更新するプロセスである。以下、その動作について説明する。

（Ｓ２５０１）更新制御手段３１４は、セキュア通信方法更新手段３１３にセキュア通信手段３１２のアップデートを、セキュア通信方法更新手段３２５にセキュア通信手段３１８のアップデートを行うように指示する。なお、ここでアップデートの指示は、所定のコマンドを送信することによって行われてもよいし、アップデート用のソフトウェアを送信することによって行われてもよい。

（Ｓ２５０２）セキュア通信方法更新手段３１３は、セキュア通信手段３１２のアップデートを、セキュア通信方法更新手段３２５は、セキュア通信手段３１８のアップデートを行う

以上で、セキュア通信方法更新プロセスの説明を終わる。

以上で、本発明の実施の形態１におけるデジタルデータ配信システムに関する説明を終わる。

（実施の形態２）

以下、本発明の実施の形態２におけるデジタルデータ配信システムについて、図面を参照しながら説明する。

実施の形態２におけるデジタルデータ配信システムは、実施の形態１におけるデジタルデータ配信システムとほぼ同一のため、ここでは実施の形態１との違いのみ明記することとし、図面においては、同一の構成要素に関しては同一の符号を付加して説明する。

図２６は、実施の形態２におけるデジタルデータ配信システムの構成を示す図である。実施の形態１のデジタルデータ配信システムと異なる点は、記録媒体アクセスアダプタ３０３内に、暗号変換手段３２１が存在せず、配信デジタルデータ記録手段３０８には、予め第二の暗号化方式によって暗号化されたデジタルデータとその復号鍵が記録されている点である。実施の形態２においては、デジタルデータ配信手段３１０は、配信デジタルデータ記録手段３０８に記録された、第二の暗号化方式によって暗号化されたデジタルデータとその復号鍵を記録媒体アクセスアダプタ３０３に送信する。また、復号鍵暗号化手段３２２は、デジタルデータ配信手段３１０から送られる復号鍵を、媒体ＩＤ検出手段３２０が検出した媒体ＩＤ３２８を利用して暗号化するものとし、媒体アクセス制御手段３２３は、デジタルデータ配信手段３１０から送られる第二の暗号化方式で暗号化されたデジタルデータと、復号鍵暗号化手段３２２が暗号化した復号鍵を、記録媒体アクセス手段３２４を制御して、記録媒体３２７に書き込むものとする。

図２７は、実施の形態２における記録媒体書き込みプロセスの動作の流れを表す。

以下、その動作について説明する。

（Ｓ２７０１）デジタルデータ配信手段３１０は、配信デジタルデータ記録手段３０８に格納されている、ダウンロード要求のあったデジタルデータを、記録媒体アクセスアダプタ３０３へ送信する。

（Ｓ２７０２）デジタルデータ配信手段３１０は、配信デジタルデータ記録手段３０８に格納されている、ダウンロード要求のあったデジタルデータに対応する復号鍵を、記録媒体アクセスアダプタ３０３へ送信する。

（Ｓ２７０３）復号鍵暗号化手段３２２は、Ｓ２７０２でデジタルデータ配信手段３１０が送信した復号鍵を、媒体ＩＤ検出手段３２０が検出した媒体ＩＤ３２８を利用して暗号化する。

（Ｓ２７０４）媒体アクセス処理制御手段３２３は、Ｓ２７０３で復号鍵暗号化手段３２２が暗号化した鍵を、記録媒体アクセス手段３２４を制御して、記録媒体３２７のセキュアデータエリア４０１に記録する。

（Ｓ２７０５）媒体アクセス処理制御手段３２３は、Ｓ２７０１でデジタルデータ配信手段３１０が送信したデジタルデータを、記録媒体アクセス手段３２４を制御して、記録媒体３２７のデータエリア４０２に記録する。

以上で、実施の形態２における記録媒体書き込みプロセスの説明を終わる。なお、記録媒体書き込みプロセス以外の動作は、実施の形態１と同様である。

以上で、実施の形態２におけるデジタルデータ配信システムの説明を終わる。

（実施の形態３）

以下、本発明の実施の形態３におけるデジタルデータ配信システムについて、図面を参照しながら説明する。

実施の形態３におけるデジタルデータ配信システムは、実施の形態２におけるデジタルデータ配信システムとほぼ同一のため、ここでは実施の形態２との違いのみ明記することとし、図面においては、同一の構成要素に関しては同一の符号を付加して説明する。

図２８は、実施の形態３におけるデジタルデータ配信システムの構成を示す図であ

る。実施の形態２のデジタルデータ配信システムと異なる点は、復号鍵暗号化手段３２２が、記録媒体アクセスアダプタ３０３内に存在せず、配信サーバー３０１内に存在する点である。配信デジタルデータ記録手段３０８には、実施の形態２同様、予め第二の暗号化方式によって暗号化されたデジタルデータとその復号鍵が記録されているものとする。実施の形態３においては、復号鍵暗号化手段３２２は、配信デジタルデータ記録手段３０８に記録された復号鍵を、媒体ＩＤ検出手段３２０から送信されてくる媒体ＩＤ３２８を利用して暗号化する。また、デジタルデータ配信手段３１０は、配信デジタルデータ記録手段３０８に記録されている、第二の暗号化方式によって暗号化されたデジタルデータと、復号鍵暗号化手段３２２が暗号化した復号鍵を記録媒体アクセスアダプタ３０３に送信する。また、媒体アクセス制御手段３２３は、デジタルデータ配信手段３１０から送られてくる、第二の暗号化方式で暗号化されたデジタルデータと媒体ＩＤ３２８を利用して暗号化された復号鍵を、記録媒体アクセス手段３２４を制御して、記録媒体３２７に書き込むものとする。

図2.9は、実施の形態２における記録媒体書き込みプロセスの動作の流れを表す。以下、その動作について説明する。

（Ｓ２９０１）デジタルデータ配信手段３１０は、配信デジタルデータ記録手段３０８に格納されている、ダウンロード要求のあったデジタルデータを、記録媒体アクセスアダプタ３０３へ送信する。

（Ｓ２９０２）復号鍵暗号化手段３２２は、配信デジタルデータ記録手段３０８に格納されている、ダウンロード要求のあったデジタルデータに対応する復号鍵を、媒体ＩＤ検出手段３２０から送られてくる媒体ＩＤ３２８を利用して暗号化する。

（Ｓ２７０３）デジタルデータ配信手段３１０は、Ｓ２９０２で復号鍵暗号化手段３２２が暗号化した復号鍵を、記録媒体アクセスアダプタ３０３へ送信する。

（Ｓ２９０４）媒体アクセス処理制御手段３２３は、Ｓ２７０３でデジタルデータ配信手段３１０が送信した復号鍵を、記録媒体アクセス手段３２４を制御して、記録媒体３２７のセキュアデータエリア４０１に記録する。

（Ｓ２７０５）媒体アクセス処理制御手段３２３は、Ｓ２７０１でデジタルデータ

配信手段３１０が送信したデジタルデータを、記録媒体アクセス手段３２４を制御して、記録媒体３２７のデータエリア４０２に記録する。

以上で、実施の形態３における記録媒体書き込みプロセスの説明を終わる。なお、記録媒体書き込みプロセス以外の動作は、実施の形態２と同様である。

以上で、実施の形態３におけるデジタルデータ配信システムの説明を終わる。

なお、実施の形態１～３において、デジタルデータとして音楽デジタルデータを例に説明したが、その他の、動画、画像、書籍、ソフトウェアなどの一般的な電子データであっても良い。

なお、実施の形態１～３において、提供されるサービスとして、ダウンロード数が無制限な購読サービスと総ダウンロード数が一定の購読サービスを例に説明したが、これに限るものでなく、履歴データベースに記録されている情報に基づいて行えるほかの条件判定に基づくサービスであってもよい。

なお、実施の形態１～３において、ブラウズ手段３１６で表示される画面を図面を用いて説明したが、これらはあくあまで一例であって、サービスの実装およびデザインに依存して異なる画面であっても良いものとする。

なお、実施の形態１～３において、記録媒体３２７は、セキュアデータエリア４０１とセキュアでないデータエリア４０２をもつ場合について説明したが、改ざん不能な媒体ＩＤ３２８を有していればセキュアデータエリア４０１を持たない記録媒体であってもよい。

なお、実施の形態１～３において、受信端末３０２は、ＳＴＢであるとしたが、それに限るものでなく、例えば、携帯電話や、パーソナルコンピューター等であってもよいものとする。

なお、実施の形態１～３において、ユーザーを認証する情報の一つとして、ユーザー名とパスワードを使用しているが、これらは、必ずしも必須でなく、アダプタＩＤ３２６のみ、または、アダプタＩＤ３２６とその他の情報との組み合わせでユーザーの認証を行ってもよいものとする。

なお、実施の形態１～３において、記録媒体アクセスアダプタ３０３内の各構成要

素は、１つのＬＳＩのなかに実装されているとしたが、例えば、図３０に示すように、必ずしも１つのＬＳＩの中に実装されている必要はない。

なお、本実施の形態１～３において、配信サーバー３０１と受信端末３０２との間の通信は、Ｃａｂｌｅを介して行われると説明したが、これに限るものでなく、インターネットや電話回線、衛星回線等、その他の通信回線であってもよいものとする。また、配信サーバー３０１から受信端末３０２への下り回線と、受信端末３０２から配信サーバー３０１への上り回線とで、異なる通信経路を使用していてもよいものとする。

以上説明した本デジタルデータ配信システムによれば、デジタルデータの権利管理を配信サーバーで行い、かつ、記録媒体へのインターフェース部分を、記録媒体へアクセスするアダプタ内で実装するため、消費者は、各々が所有する受信端末に、各サービス用のアダプタを接続することで、各種サービスを受信することが可能となる。また、デジタルデータ配信サービス提供業者は、新サービスを開始する際、そのサービス用のアダプタを提供することによって、構成の異なる複数の受信端末が存在する場合にも、その構成の違いを気にすることなく、サービスを開始することができるようになる。また、受信端末製造・販売業者にとっては、受信端末内に、タンパレジスタント技術を施す必要がなくなり、受信端末の開発が容易になる。また、その為、受信端末の価格をおさえることができる。